

# Integrating the NEDSS Base System With a Directory Service: Authentication and Authorization Eccentricities in a State Health Department With Different Security Requirements

June Bancroft, MPH  
Epidemiologist

# Data Security and Public Health

- Public health exemptions for sharing data
- Health insurance portability and accountability act (HIPAA)
- Public health information network
- eGovernment initiative – electronic medical records

# Authorization

- Authorization is finding out if the person, once identified, is permitted to have the resource. This is usually determined by finding out if that person is a part of a particular group.

# Authentication

- The verification of the identity of a person; That they are who they claim they are – generally a username and password

# Access Control

- Access control allows you to restrict access based on criteria unrelated to the identity of the user
- Role based access control (also called role based security) has become the predominant model because it reduces the complexity and cost of security administration

# CDC Guidance...Systems Developed or Promoted Will...

- Support standards-based access to major database management system
- Use the same implementation environment wherever possible, will be sensitive to multiple operating and database management systems that exist at state and local levels
- Use single data and vocabulary standards, wherever possible, to describe the same data elements

# Further CDC guidance ... systems will...

- Integrate into existing state or local strong authentication and authorization technologies
- Use a common methodology for the exchange of data between partner systems (ebXML, SOAP, HTTPS)
- Require only one single directory of public health, clinical and participant personnel (LDAP directory)

# PHIN Functions and Specifications

- Client and server X.509 digital certificates or comparable strong authentication methodology
- Use role-based, mandatory access control protocols
- Security patches and configuration corrections should be applied promptly



# More PHIN Functions and Specifications

- Provide routine virus scanning, intrusion detection, network vulnerability analysis
- Access and control of data thru selective integrated repository authorization
- An encryption engine and appropriate use of encrypted data
- Access control through a firewall

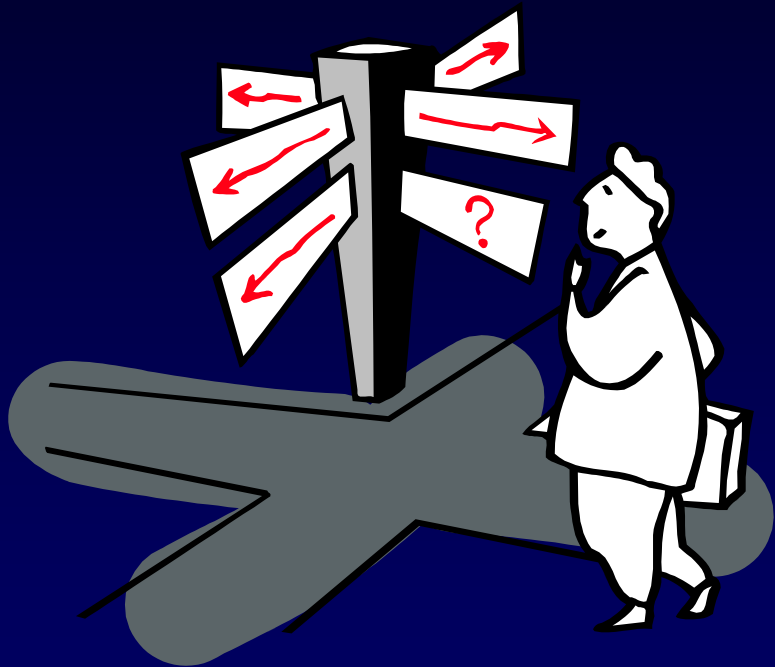
# Oregon Considerations for the NBS

- Oregon's IT infrastructure did not meet these specifications
- Enterprise LDAP directory service was in planning stages
- First web-based reporting system in State public Health
- Other NBS sites were using an intranet
- NBS has no built in Authentication

# Oregon Systems Using Directory Like Information

- eSentinel – hospital web-based reporting of cases of public health concern
- Health Alert Network – web-based communication tool for LHDs
- Alert Oregon – web-based role centered 24/7 alerting application
- Electronic lab reporting –sFTP – labs and physicians who order tests

# Other options were considered



- Prior troubles with Virtual Private Networks and Local Health Departments
- Digital Certificates
- Key fobs, etc.

# Oregon Solution

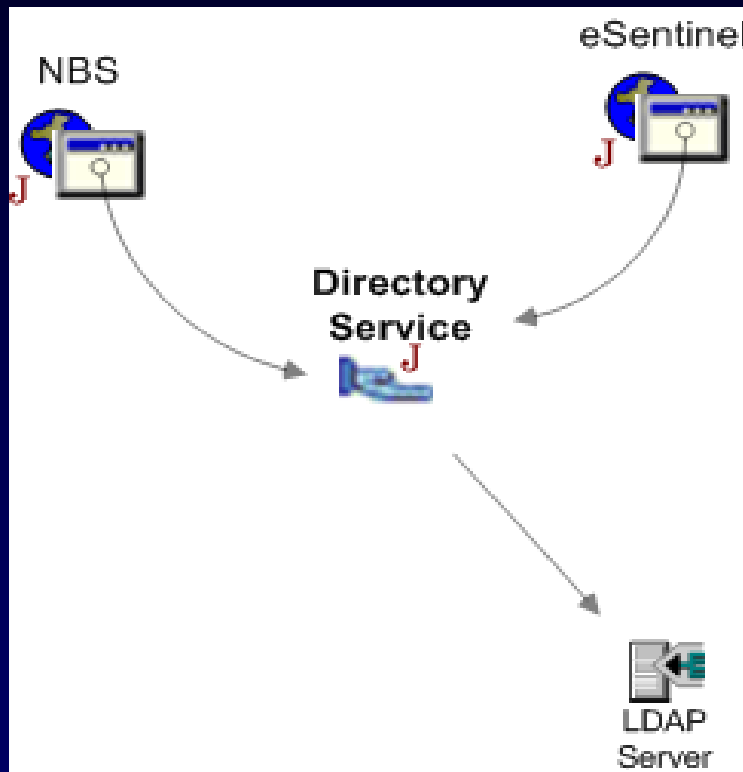
## Part 1

- NBS designers provide an ability to hook into an external java class that will integrate with a our planned Enterprise authentication.

## Part 2

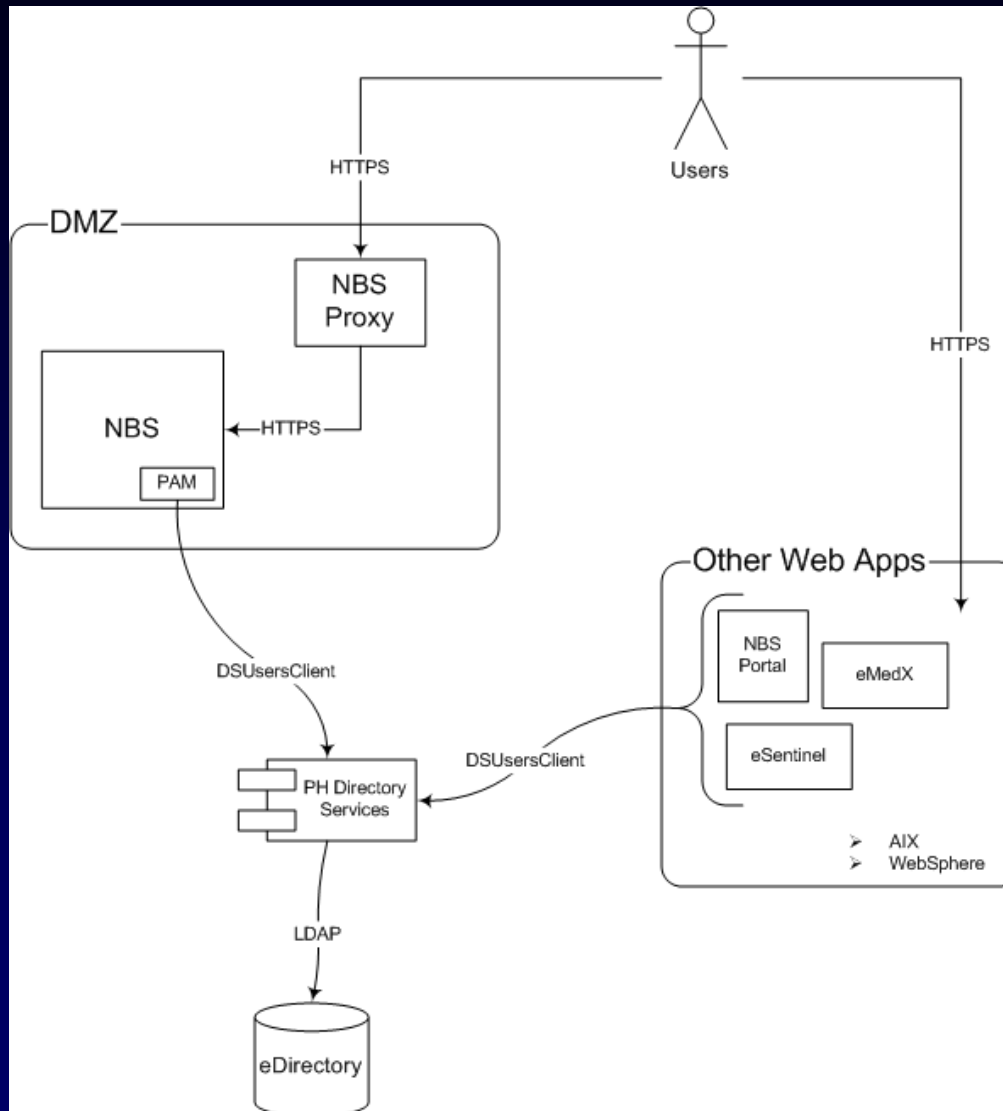
- Build and test a simple authentication module and plug it into the NBS without having to develop that module on WebLogic

# Integrated solution



- Single sign on
- Role-based application access
- Quasi 2-factor authentication
- Standardized java API for application access

# High Level Authorization



# System Perplexities

- Peripheral activities of the authentication process.
  - How do you handle situations where a user's password has expired, been suspended due to failed logon attempt, etc.
- To avoid creating a NBS development environment using non-state standards - all peripheral activities were built in WebSphere



# Limitations

- Access Control interface was built in a way that makes the NBS incompatible for single sign-on between the NBS and other applications
- Murky waters in knowing where the system breaks down


# Application Manager

NBS Application Manager - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address <https://apps.dhs.state.or.us/eNBSAuth/logon>




**DHS EXTRANET**  
Oregon Department of Human Services  
**NBS Application Manager**

[eSENTINEL](#) [HAN](#)


[Log Out](#) [Log into Manager](#) [Change Question & Response](#) [Change Password](#)

[NBS](#)  
[Contact](#)  
[Help](#)

eNBSAuth  
V 1.0



*Welcome  
to the Oregon DHS Portal website  
for the  
NEDSS  
Base System*



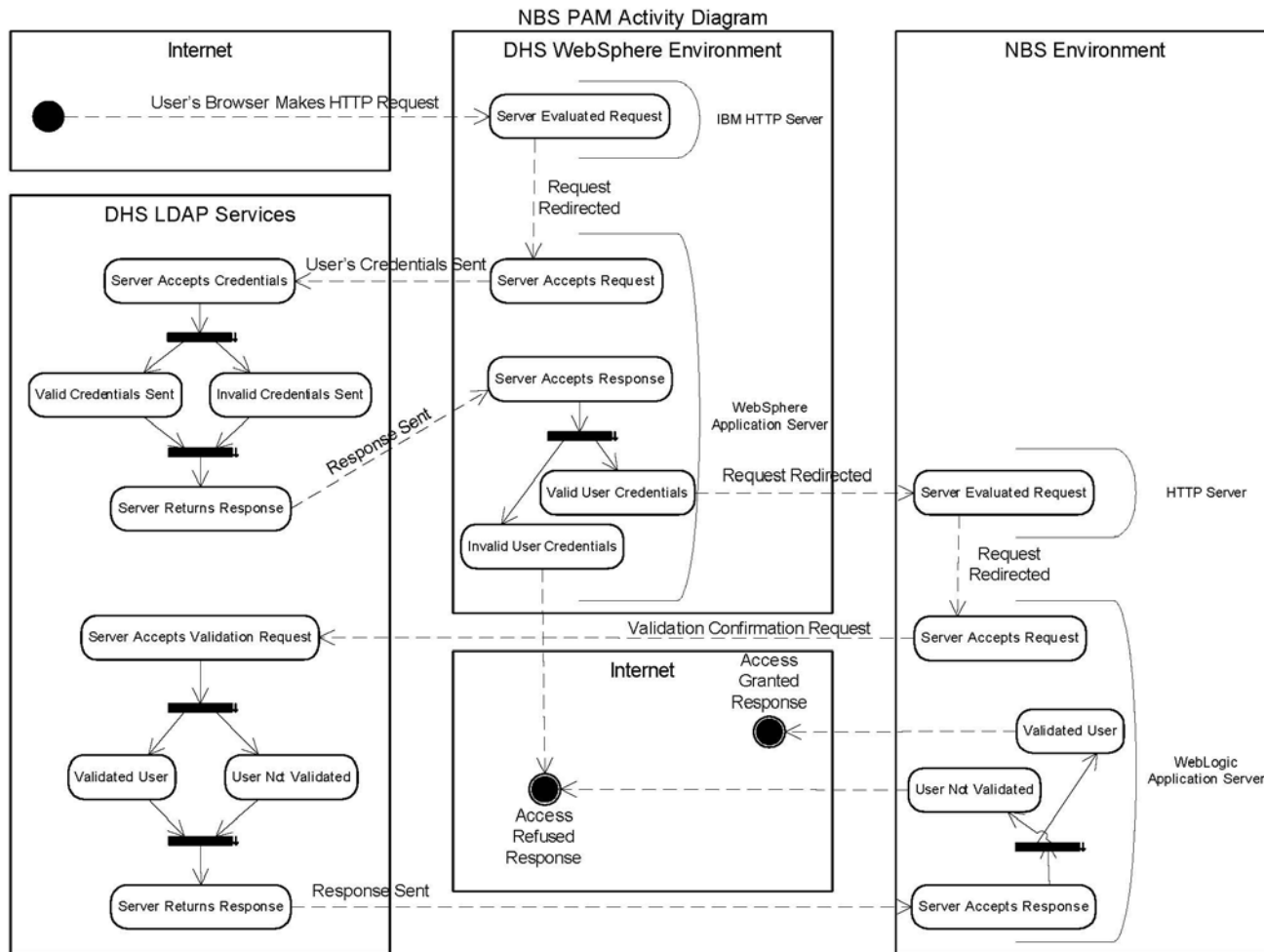
---

You are entering a secure site for reporting cases of public health significance.  
( <http://www.healthoregon.org/acd/oars/div18.cfm> ).  
[Post-Production Release Notes](#)

# Like Solving a Puzzle

- Built by one shop, installed by another, maintained by yet another
  - is it a server issue, IP address issue?
- Where does the traffic flow or jam up— through Websphere and NBS or in the redirect?
- Which application (Websphere or WebLogic) timed out?

# Authorization Details



# Space/time vortex

- Authorization token refreshes unless queried
  - NBS doesn't know to go back to the application manager
- LDAP server could shut down session but hold onto object – resulting in a rejected user

# More Time Vacuums ...

- Secure socket layer (SSL) connectivity
  - We have 3-level certificates, WebLogic has 2
  - 30-day trial certificate while wait for permanent one
    - Another piece added to the puzzle???
  - Jumping from one SSL cert to another invalidates SSL session user originally validated in!

# Two dimensional administration

- Maintain a user in authentication application: LDAP directory
- Maintain a user in NBS
  - Same userid – authentication application passes ok to NBS – this is a valid user

# NBS administration

- Customized to meet Oregon business needs
  - Epidemiologists work across program area modules used by NBS
  - Almost every condition is a program area
  - Program area – condition mapping forms critical linkages inside NBS application
  - Increases complexity of NBS system administration



# Trade offs

- Complex system administration, but user is not overwhelmed by information on the home page
- Eases routing of information to appropriate individuals
- Requires multiple log in names based on what doing for that day?
  - Epi on call with access to all
  - Reviewing specific investigations/lab reports

# Overview of NBS Administration

- Master system administrator
- Program area administrator
- Permissions sets
  - Linked to role, conditions and jurisdictions
  - Control what a user can do – add providers, edit records, etc

# NBS definitions

- A role is an organizational classification that describes operational functions and responsibilities  
Users' roles define
  - the screens they can access
  - the operations they can perform in those screens
  - the program areas and jurisdictions to which they have access
- A Program Area is an organizational entity responsible for Public Health management of a specific set of disease conditions,
- Jurisdiction is an organization responsible for Public Health activities within a defined geographic area.

# Interactions between the NBS & Application manager

- Controls what user can see and do within systems
  - Unknowns around whether person had right role and permission sets – is the application working properly?
- Complicates upgrades 1.1.1 to 1.1.3 – SP1, SP2, Hot fix 1, 2 ...

# Jurisdictional Hurdles

- One Pilot County
  - Required creation of additional permission set to allow them to use system
  - Each Local Health Department addition
    - Another permission set?? (30 program areas x35 local health departments=1,050 permission sets!!)

# Next Steps

- Revisit solution and find other ways to implement authentication so that we have single sign on that is compatible with all applications (Health Alert Network, eSentinel, eMed-X, etc)
- Have a shared directory for all PHIN related applications

# Additional Steps

- Formally evaluate NBS fit in Oregon
  - Message Oregon ELR data into the NBS
- Expand to other Local Health Departments as appropriate

# Acknowledgements

- Computer Science Corporation - Vydianath Iyer (Iyer) & Iyer again
- Oregon NEDSS Team – Robert Barker, Tom Chen, Walt Davis, Dave O’Neill, Boris Shternberg
- Oregon Health Services - Michelle Barber